Please replace the paragraph on page 7, lines 7 to 15 with the following paragraph.

a2)

-- The device P(C) delivers a serial number S(C) at each transaction, and S(C) can be read off P(C) only in the presence of customer C. For more privacy, it would be better that P(C) generates numbers S(C,n), where n is an integer belonging to a large set {1,2,...,N}. Then, for each new insurance company and or other partner of customer C, a new number n is chosen as a starting number for all further transaction(s) between the two parties. In particular, if C quits insurance entity I for another company and comes back to I, it can change the n associated to I. For simplicity, the use of this number n will be omitted in the sequel, as using it is a trivial amelioration of the overall protocol. –

Please replace the paragraph on page 7, line 16 to page 8, line 4, with the following paragraph.

a3

-- The insurance entity I will also choose a large set of verifiers Vj, j=1, 2,... which will be medical practitioners for health (or life) insurance, and garages in the case of automobile insurance. Any verifier will be equipped with the apparatus needed to verify portable devices as described above, and will be connected to the Internet so that they can send information to third party T. The relation with T can be performed using a privacy protection mechanism, involving several other parties to avoid possible collusion, as described for instance in the home page of the NetBill Security and Transaction Protocol by B. Cox, J.D. Tygar, an M. Sirbu which can be obtained on the Internet at www.ini.cmu.edu/netbill: see the paper "Maintaining privacy in electronic transactions" by Benjamin T.H. Fox. These are referred to collectively as "Ref3". –

Please replace the paragraph on page 8, lines 5 to 14 with the following paragraph.

a4

-- When deciding to register with insurance I, customer C sends to T an application A. This application can be taken off, for example, the world-wide-web (WWW) page of the business (insurance) entity I, together with a piece of software SOFT, such as a JAVA applet, which allows encryption using pu1(I) where (Pr1(I),pu1(I)) is the public signature scheme of I. SOFT also allows customer C to compute a public signature scheme (Pr2(I,C),pu2(I,C)). C will